UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,679	04/02/2004	Robert Thomas Owen Rees	300202358-2	9742

7590 09/13/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,679	REES, ROBERT THOMAS OWEN	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/20/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 16 objected to because of the following informalities:

Claim 16 contains the statement "providing the trusted party with the its public key" (emphasis added).

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 10, 14, 17, and 23-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Stone et al. (U.S. Pub. No. 2002/0080964 A1), hereinafter "Stone".

Referring to claims 1, 23:

Stone teaches:

A method of passing data securely from an originator to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for receipt of the data (see figure 5, element 2 'seller client'; and page3, paragraph [0062] of Stone);

the originator selecting a trusted party (see figure 5, element 1 'transaction server'; and page3, paragraph [0062] of Stone);

the originator selecting a first key without reference to the condition (see page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added);

the originator encrypting the data using the first key (see page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added);

the originator making the condition, and the encrypted data available to the recipient (see page 4, paragraph [0067], lines 12-17 of Stone);

the recipient providing the trusted party with evidence that it meets the condition (see figure 9; and page 4, paragraph [0075] of Stone),

the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient (see figure 9; and page 4, paragraph [0075] of Stone), and

the recipient decrypting the data using the first key (see figure 9; and page 4, paragraph [0075] of Stone).

Referring to claims 10, 24:

Stone teaches:

A method for an originator to make data available securely to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for receipt of the data (see figure 5, element 2 'seller client'; and page3, paragraph [0062] of Stone);

the originator selecting a trusted party (see figure 5, element 1 'transaction server'; and page3, paragraph [0062] of Stone);

the originator selecting a first key without reference to the condition (see

page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added);

the originator encrypting the data using the first key (see page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added);

the originator making the condition, and the encrypted data available to the recipient (see page 4, paragraph [0067], lines 12-17 of Stone).

Referring to claims 14, 25:

Stone teaches:

A method for a recipient to receive data made available securely by an originator, who has selected a trusted party to be involved, comprising the steps of:

Obtaining a condition for decryption of the data set by the originator and the data encrypted using a first key generated without reference to the condition (see page 4, paragraph [0067], lines 12-17 of Stone);

providing the trusted party with evidence that it meets the condition (see figure 9; and page 4, paragraph [0075] of Stone),

receiving the first key for decryption of the data from the trusted party (see figure 9; and page 4, paragraph [0075] of Stone), and

decrypting the data using the first key (see figure 9; and page 4, paragraph [0075] of Stone).

Referring to claims 17, 26:

Stone teaches:

A method for a trusted party to facilitate the passing of data securely from an originator to a recipient, comprising the steps of:

Receiving from the recipient evidence that they meet the condition (see figure 9; and page 4, paragraph [0075] of Stone),

comparing the evidence against the condition to confirm that the recipient does meet the condition (see figure 9; and page 4, paragraph [0075] of Stone), and

if the recipient meets the condition, providing the first key to the recipient (see figure 9; and page 4, paragraph [0075] of Stone).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2-9, 11-13, 15-16, 18-22, 27-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stone et al. (U.S. Pub. No. 2002/0080964 A1) in view of Voshiura et al. (U.S. Patent No. 6,131,162), hereinafter "Voshiura".

Referring to claims 2, 11, 15-16, 18, 20:

i. Stone teaches the claimed subject matter: a method of passing data securely from an originator to a recipient (see claim 1 above). Stone discloses the encryption and the decryption (see page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added). However, Stone does not specially mention the asymmetrical key pair.

ii. Voshiura teaches a content distribution system, wherein Voshiura discloses the asymmetrical key pair and its usage: "This invention also provides a content distribution system wherein the encrypting apparatus of the distribution system encrypts the content using the public key of the user of the receiving system and the decrypting apparatus of the receiving system decrypts the content encrypted using the

private key of the user of the distribution system." (see column 8, lines 54-59 of Voshiura, emphasis added).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Voshiura into the method of Stone to use the asymmetrical key pair for encrypting the data to be distributed in a content distribution system.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Voshiura into the system of Stone to use the asymmetrical key pair for encrypting the data to be distributed in a content distribution system, because it's well known in the art that asymmetrical key pair is used for data encryption to ensure data security.

Referring to claims 3-4, 6, 12, 19, 22, 28-29:

Stone and Voshiura teach the claimed subject matter: a method of passing data securely from an originator to a recipient (see claim 1 above). They further disclose encrypting with the public key and the decrypting with the private key (see column 8, lines 54-59 of Stone).

Referring to claim 5:

Stone and Voshiura teach the claimed subject matter: a method of passing data securely from an originator to a recipient (see claim 1 above). They further disclose the steps of:

The originator providing the condition to the trusted party (see figure 5, element 2 'seller client'; and page3, paragraph [0062] of Stone);

the trusted party storing the condition and the asymmetric key pair (see figure 5, element 2 'seller client'; and page3, paragraph [0062] of Stone);

the recipient providing the trusted party with evidence that it meets the condition see figure 5, element 2 'seller client'; and page3, paragraph [0062] of Stone);

the trusted party retrieving the condition and asymmetric key pair from store, and satisfying itself that the recipient meets the condition (see figure 9; and page 4, paragraph [0075] of Stone), and

the trusted party providing the decrypting key of the asymmetric key pair

to the recipient to act as a decrypting first key (see figure 9; and page 4, paragraph [0075] of Stone).

Referring to claim 7:

Stone and Voshiura teach the claimed subject matter: a method of passing data securely from an originator to a recipient (see claim 1 above). They further disclose that at the time the originator encrypts the data the recipient is unknown to them (see page 1, paragraph [0013] of Stone).

Referring to claim 8:

Stone and Voshiura teach the claimed subject matter: a method of passing data securely from an originator to a recipient (see claim 1 above). They further disclose the publishing and storing (see page 5, paragraph [0089] of Stone).

Referring to claim 9:

Stone and Voshiura teach the claimed subject matter: a method of passing data securely from an originator to a recipient (see claim 1 above). They further disclose the storage medium (see page 5, paragraph [0088] of Stone).

Referring to claims 13, 30:

Stone and Voshiura teach the claimed subject matter: a method for an originator to make data available securely to a recipient (see claim 10 above). They further disclose generating an asymmetrical key pair (see column 13, lines 1-5 of Voshiura).

Referring to claim 21:

Stone and Voshiura teach the claimed subject matter: a method for a trusted party to facilitate the passing of data securely from an originator to a recipient (see claim 17 above). They further disclose the additional steps of:

receiving the condition from the originator (see page 4, paragraph [0073] of Stone);

storing the condition and the asymmetric first key pair (see page 4, paragraph [0073] of Stone);

upon receipt of the evidence from the recipient that they meet the condition, retrieving the condition and asymmetric first key pair from store before

comparing the evidence against the condition to confirm that the recipient does meet the condition (see page 4, paragraph [0073] of Stone), and

providing to the recipient the decrypting key of the asymmetric first key pair to act as a decrypting first key originator (see page 4, paragraph [0073] of Stone).

Referring to claim 27:

i. Stone teaches:

A computer system for passing data securely from an originator to a recipient comprising a first computer entity associated with the originator, a second computer entity associated with the recipient and a third computer entity associated with a trusted party, there being communication means between the first computer entity and the second computer entity and between the second computer entity and the third computer entity (see figure 1 of Stone),

the first computer entity selecting a condition to be met by the recipient before receipt of the data and a first key generated without reference to the condition, and encrypting the data with that first key, and making available to the second computer entity (see page 3, paragraph [0062] of Stone);

the second computer entity being arranged to forward evidence that the recipient meets the condition to the third computer entity (see page 4, paragraph [0075] of Stone), and

the third computer entity being arranged to compare the evidence with the condition and if satisfied that the recipient meets the condition to provide the first key to the second computer entity for decryption of the data (see page 4, paragraph [0075] of Stone).

Stone discloses the encryption and the decryption (see page 4, paragraph [0075] 'decryption keys'; and paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added). However, Stone does not specially mention the asymmetrical key pair consisting of the public key and the private key.

ii. Voshiura teaches a content distribution system, wherein Voshiura discloses the asymmetrical key pair and its usage: "This invention also provides a

content distribution system wherein the encrypting apparatus of the distribution system encrypts the content using the public key of the user of the receiving system and the decrypting apparatus of the receiving system decrypts the content encrypted using the private key of the user of the distribution system." (see column 8, lines 54-59 of Voshiura, emphasis added).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Voshiura into the method of Stone to use the asymmetrical key pair for encrypting the data to be distributed in a content distribution system.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Voshiura into the system of Stone to use the asymmetrical key pair for encrypting the data to be distributed in a content distribution system, because it's well known in the art that asymmetrical key pair is used for data encryption to ensure data security.

Referring to claim 31:

i. Stone teaches:

A method of passing data securely from an originator to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for decryption of the data (see figure 5, element 2 'seller client'; and page3, paragraph [0062] of Stone);

the originator selecting a first key without reference to the condition (see page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added);

the originator encrypting the data using the first key (see page 4, paragraph [0075] 'decryption keys'; paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added);

the originator making the condition, and the encrypted data available to the recipient (see page 4, paragraph [0067], lines 12-17 of Stone);

upon receipt by the trusted party of the recipient's evidence that the

recipient meets the condition, the trusted party satisfies itself that the recipient meets the condition, provides the first key to the recipient (see figure 9; and page 4, paragraph [0075] of Stone), and

the recipient decrypts the data using the first key (see figure 9; and page 4, paragraph [0075] of Stone).

Stone discloses the encryption and the decryption (see page 4, paragraph [0075] 'decryption keys'; and paragraph [0083] 'Data may be carried on other carriers preferably in encryption form for security' of Stone, emphasis added). However, Stone does not specially mention the asymmetrical key pair consisting of the public key and the private key.

ii. Voshiura teaches a content distribution system, wherein Voshiura discloses the asymmetrical key pair and its usage: "This invention also provides a content distribution system wherein the encrypting apparatus of the distribution system encrypts the content using the public key of the user of the receiving system and the decrypting apparatus of the receiving system decrypts the content encrypted using the private key of the user of the distribution system." (see column 8, lines 54-59 of Voshiura, emphasis added).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Voshiura into the method of Stone to use the asymmetrical key pair for encrypting the data to be distributed in a content distribution system.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Voshiura into the system of Stone to use the asymmetrical key pair for encrypting the data to be distributed in a content distribution system, because it's well known in the art that asymmetrical key pair is used for data encryption to ensure data security.

Referring to claim 32:

Stone and Voshiura teach the claimed subject matter: a method of passing data securely from an originator to a recipient. They further disclose generating an symmetrical key pair (see column 1, lines 56-58 of Voshiura).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
August 30, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100